Abstract

The fourth generation technology of broadband wireless networks i.e. WiMAX (Worldwide Interoperability for Microwave Access) became popular due to its features like high speed internet access, large coverage area and interoperability for different type of devices. Non-Line-of-sight propagation with lower frequency improvement makes WiMAX vulnerable to various security threats. Hence, authentication and authorization are used for protecting network from various attacks. Although there are standard authentication protocols in IEEE 802.16, but still WiMAX is vulnerable to attacks such as replay attack, DoS (denial of service attack), interleaving attack etc. In this paper, an exhaustive analysis of existing solutions in standard PKMv2 (privacy key management version 2) protocol is presented. The Proxy Base Station based authentication protocol addresses the major attacks namely DoS attack, interleaving...
Proxy Base Station based Authentication Protocol for Broadband Wireless Network

attack, replay attack and downgrade attack. With the introduction of PS (proxy base station), the task of validation is distributed between the PS and BS (base station), it resolves the DoS attack due to the resource exhausting validation procedure [23]. Our proposed authentication protocol is modeled and verified on CPN (Colored PetriNet) tool (version 3. 0. 2)[1, 2] with and without intruder and compared with PKMv2 standard protocol. The state space analysis report for standard verification parameters shows that our proposed protocol satisfies the desired properties of liveness and fairness with negligible overheads and it is secure and efficient.

References

- WiMAX Forum, Fixed, Nomadic, Portable and Mobile Applications for 802. 16-2004 and 802. 16e WiMAX (Nov. 2005).
- Wenbo Mao, "Modern Cryptography: Theory and Practice," Pearson
Proxy Base Station based Authentication Protocol for Broadband Wireless Network


Index Terms

Computer Science Wireless
Keywords
WiMAX  Authentication  Proxy  Base station  protocol  Privacy and key management